

**פתרונות תרגיל 1-רשתות תקשורת**  
**מגיישם-אבי סימפסון(00) (205789100) יקיר פנהס (203200530)**

**שאלה 1**  
**סעיף א**

The screenshot shows a Linux desktop environment with a terminal window titled 'untitled' containing Python code for a UDP server. The code sends messages to a client and receives responses. A second terminal window shows the client's response. A file manager window is also visible.

**Terminal 1 (Left):**

```
avi@avi-Lenovo-Flex-2-15:~/PycharmProjects/untitled$ python UDPserver.py
Message: helloworld!!!! from: ('127.0.0.1', 48421)
Message: hi from: ('127.0.0.1', 48421)
Message: hi from: ('127.0.0.1', 48421)
Message: hi again from: ('127.0.0.1', 48421)
```

**Terminal 2 (Right):**

```
avi@avi-Lenovo-Flex-2-15:~/PycharmProjects/untitled$ python UDPClient.py
Message to send: helloworld!!!!!
Server sent: HELLOWORLD!!!!!!
Message to send: hi
Server sent: HI
Message to send: hi
Server sent: HI
Message to send: hi again
Server sent: HI AGAIN
Message to send: 
```

**סעיף ב**  
CLIENT

untitled - [~/PycharmProjects/untitled]

File Edit View Navigate Code Refactor Run Tools VCS Window Help

untitled > UDPClient.py

UDPServer.py x UDPClient.py x

```
1 #ייבוא של פונקציה ומשתנים מספורית SOCKET
2 s = socket(AF_INET, SOCK_DGRAM) #יצירת הocket לثان המשתנה s
3 dest_ip = '127.0.0.1' #הדקן שללי רץ השירות
4 dest_port = 12345 #הפורט שללי רץ השירות
5 msg = raw_input("Message to send: ") #הUSER מכניס קלט למערכת שוכנס למשתנה msg.
6 while not msg == 'quit': quit #וללאה שתרוץ עד שהליקוט ישלה לשרת PORT
7     s.sendto(msg, (dest_ip,dest_port)) #פונקציה שלוחת לשרת את הודעה דרכ שימוש בIP
8     data, sender_info = s.recvfrom(2048) #קבלת הודעה לثان משתנה DATA כאשר זהות השולח נמצאת בENDERINFO
9     print "Server sent: ", data #הדףת הודעה שהתקבלה בשורה הקודמת
10    msg = raw_input("Message to send: ") #הUSER מכניס קלט חדש
11    s.close() #סגירת ערך התקשורת
12
```

**SERVER**

untitled - [~/PycharmProjects/untitled]

File Edit View Navigate Code Refactor Run Tools VCS Window Help

untitled > UDPServer.py

UDPServer.py x UDPClient.py x

```
1 #ייבוא של פונקציה ומשתנים מספורית SOCKET
2 s = socket(AF_INET, SOCK_DGRAM) #יצירת הocket SOCKET לثان המשתנה s
3 source_ip = '0.0.0.0' #הנקה של השירות
4 source_port = 12345 #הPORT במחשב עליה רץ השירות
5 s.bind((source_ip, source_port)) #יצירת ערך האזנה של השירות
6 while True: #וללאה איןסוףות לתוכנת
7     data, sender_info = s.recvfrom(2048) #קבלת הודעה מלקוח CLIENT מטעם לثان DATA ואת פרטיו CLIENT שמם בENDERINFO
8     print "Message: ", data, " from: ", sender_info #הדףת הודעה ופרטי הלקוח CLIENT
9     s.sendto(data.upper(), sender_info) #שליחת הודעה באותיות גדולות תורה CLIENT
```

## שאלה 2

### סעיף א

\*enp0s3

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
14265	125.416414278	198.255.112.234	10.0.2.15	TCP	60	443 → 59794 [ACK] Seq=5811 Ack=611 Win=65535 Len=0
14266	125.423314120	10.0.2.15	209.58.130.220	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
14267	125.423823798	209.58.130.220	10.0.2.15	TCP	60	443 → 36690 [ACK] Seq=5811 Ack=611 Win=65535 Len=0
14268	125.432154985	10.0.2.15	198.255.112.234	TLSv1.2	642	Application Data
14269	125.432576279	198.255.112.234	10.0.2.15	TCP	60	443 → 59794 [ACK] Seq=5811 Ack=1199 Win=65535 Len=0
14270	125.432758128	10.0.2.15	209.58.130.220	TLSv1.2	1167	Application Data
14271	125.433094669	209.58.130.220	10.0.2.15	TCP	60	443 → 36690 [ACK] Seq=5811 Ack=1724 Win=65535 Len=0

Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0

Ethernet II, Src: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.0.77.32

Transmission Control Protocol, Src Port: 34520, Dst Port: 443, Seq: 1, Ack: 1, Len: 39

Secure Sockets Layer

```
0000  52 54 00 12 35 02 08 00 27 8b 4b c5 08 00 45 00  RT..5...'.K..E.
0010  00 4f 8e dd 40 00 40 06 92 9c 0a 00 02 0f c0 00  .O..@..@. .....
0020  4d 20 86 d8 01 bb f5 2a 3b b1 0c 24 a4 86 50 18  M.....* ;..$.P.
0030  ff 28 19 71 00 00 17 03 03 00 22 40 3b 45 09 5b  .( q.... '@;E.[
0040  9d 98 80 c7 5a 0a 3e f2 17 3e 79 17 76 4a 44 75  ....Z.> .>y.vJDu
0050  c2 d0 ee 0a 3b 6d e3 5b 22 b4 3f 42 38  ....;m.[ ".?B8
```

wireshark\_enp0s3\_20181107165626\_IUzbRR.pcapng

Packets: 14271 · Displayed: 14271 (100.0%) · Profile: Default

מספר החבילות שהושנפו הוא 14,271

### סעיף ב

\*enp0s3

udp

No.	Time	Source	Destination	Protocol	Length	Info
36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.679943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAM...

Frame 36: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

Ethernet II, Src: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 132.70.60.124

User Datagram Protocol, Src Port: 45651, Dst Port: 53

Domain Name System (query)

```
0000  52 54 00 12 35 02 08 00 27 8b 4b c5 08 00 45 00  RT..5...'.K..E.
0010  00 3f 33 fc 40 00 40 11 39 e1 0a 00 02 0f 84 46  .?3..@..9.....F
0020  3c 7c b2 53 00 35 00 2b cd 0d 70 cc 01 00 00 01  <| S..5+ ..p.....
0030  00 00 00 00 00 04 6f 63 73 70 08 64 69 67 69  .....o csp-digi
0040  63 65 72 74 03 63 6f 6d 00 00 01 00 01  cert.com .....
```

User Datagram Protocol: Protocol

Packets: 14271 · Displayed: 838 (5.9%) · Dropped: 0 (0.0%) · Profile: Default

לאחר סינון נשארו 838 תוצאות עבור udp

Terminal

```
ubuntu@ubuntu-VirtualBox:~$ ifconfig
enp0s3  Link encap:Ethernet HWaddr 08:00:27:8b:4b:c5
        inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
              inet6 addr: fe80::1569:9ebf:a7df:8aae/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:72872 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:33530 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:62173268 (62.1 MB) TX bytes:3356893 (3.3 MB)

lo    Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
              inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING MTU:65536 Metric:1
                  RX packets:2456 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:2456 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:250501 (250.5 KB) TX bytes:250501 (250.5 KB)

ubuntu@ubuntu-VirtualBox:~$
```

Frame 30: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
 ▶ Ethernet II, Src: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 132.70.60.124
 ▶ User Datagram Protocol, Src Port: 45651, Dst Port: 53
 ▶ Domain Name System (query)

0000	52	54	00	12	35	02	08	00	27	8b	4b	c5	08	00	45	00	RT...5...	'K..E.
0010	00	3f	33	fc	40	00	40	11	39	e1	0a	00	02	0f	84	46	.?3 @. @.	9.....F
0020	3c	7c	b2	53	00	35	00	2b	cd	0d	70	cc	01	00	00	01	<  S.5.+	.p....
0030	00	00	00	00	00	00	04	6f	63	73	70	08	64	69	67	69	.....o	csp.digi
0040	63	65	72	74	03	63	6f	6d	00	00	01	00	01				cert.com	.....

User Datagram Protocol: Protocol

Packets: 14271 · Displayed: 838 (5.9%) · Dropped: 0 (0.0%) · Profile: Default

כתובת האייפי שהשתמשו בה בתרגיל היא 10.0.2.15

\*enp0s3

dns

No.	Time	Source	Destination	Protocol	Length	Info
36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.679943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAME...

Frame 37: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
 ▶ Ethernet II, Src: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 132.70.9.100
 ▶ User Datagram Protocol, Src Port: 45651, Dst Port: 53
 ▶ Domain Name System (query)

0000	52	54	00	12	35	02	08	00	27	8b	4b	c5	08	00	45	00	RT...5...	'K..E.
0010	00	3f	8f	26	40	00	40	11	11	cf	0a	00	02	0f	84	46	.? &@. @.	. ....F
0020	09	64	b2	53	00	35	00	2b	99	f5	70	cc	01	00	00	01	.d S.5.+	.p....
0030	00	00	00	00	00	00	04	6f	63	73	70	08	64	69	67	69	.....o	csp.digi
0040	63	65	72	74	03	63	6f	6d	00	00	01	00	01				cert.com	.....

Domain Name System: Protocol

Packets: 14271 · Displayed: 838 (5.9%) · Dropped: 0 (0.0%) · Profile: Default

החבריה נשלחה מהמחשב שלנו כי כתובת האייפי של המקור היא הכתובת מסעיף ג

\*enp0s3

**dns**

No.	Time	Source	Destination	Protocol	Length	Info
36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.679943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAM...

Frame 37: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

Ethernet II, Src: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 132.70.9.100

User Datagram Protocol, Src Port: 45651, Dst Port: 53

Domain Name System (query)

```
0000  52 54 00 12 35 02 08 00 27 8b 4b c5 08 00 45 00  RT-5... 'K..E.
0010  00 3f 8f 26 40 00 40 11 11 cf 0a 00 02 0f 84 46  .?&@. ....F
0020  09 64 b2 53 00 35 00 2b 99 f5 70 cc 01 00 00 01  .d-S-5+ ..p...
0030  00 00 00 00 00 04 6f 63 73 70 08 64 69 67 69  .....o csp-digi
0040  63 65 72 74 03 63 6f 6d 00 00 01 00 01  cert.com ....
```

User Datagram Protocol (udp), 8 bytes

Packets: 14271 · Displayed: 838 (5.9%) · Dropped: 0 (0.0%) · Profile: Default

הפורט ממנו נשלחה החבילה שהוא הפורט של הלוקה הוא 45651  
הפורט אליו נשלחה החבילה שהוא פорт השרת הוא פорт 53

\*enp0s3

**dns**

No.	Time	Source	Destination	Protocol	Length	Info
36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.679943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAM...

Frame 37: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

Ethernet II, Src: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 132.70.9.100

User Datagram Protocol, Src Port: 45651, Dst Port: 53

Domain Name System (query)

```
0000  52 54 00 12 35 02 08 00 27 8b 4b c5 08 00 45 00  RT-5... 'K..E.
0010  00 3f 8f 26 40 00 40 11 11 cf 0a 00 02 0f 84 46  .?&@. ....F
0020  09 64 b2 53 00 35 00 2b 99 f5 70 cc 01 00 00 01  .d-S-5+ ..p...
0030  00 00 00 00 00 04 6f 63 73 70 08 64 69 67 69  .....o csp-digi
0040  63 65 72 74 03 63 6f 6d 00 00 01 00 01  cert.com ....
```

Bytes 44-45: Non-authenticated data (dns.flags.checkdisable)

Packets: 14271 · Displayed: 838 (5.9%) · Dropped: 0 (0.0%) · Profile: Default

האיפי ממנו נשלחה החבילה הוא 10.0.2.15  
האיפי אליו נשלחה החבילה הוא 132.70.9.100

\*enp0s3

**dns**

No.	Time	Source	Destination	Protocol	Length	Info
36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.6779943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAM...

Frame 37: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

Ethernet II, Src: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 132.70.9.100

User Datagram Protocol, Src Port: 45651, Dst Port: 53

Domain Name System (query)

```
0000  52 54 00 12 35 02 08 00 27 8b 4b c5 08 00 45 00  RT..5...'.K..E.
0010  00 3f 8f 26 40 00 40 11 11 cf 0a 00 02 0f 84 46  .?&@.0. ....F
0020  09 64 b2 53 00 35 00 2b 99 f5 70 cc 01 00 00 01  .d S-5.+ p.....
0030  00 00 00 00 00 04 6f 63 73 70 08 64 69 67 69  .....o csp-digi
0040  63 65 72 74 03 63 6f 6d 00 00 01 00 01 cert.com .....
```

Ethernet (eth), 14 bytes

Packets: 14271 · Displayed: 838 (5.9%) · Dropped: 0 (0.0%) · Profile: Default

SRC MAC-08:00:27:8b:4b:c5  
DST MAC-52:54:00:12:35:02

### סעיף ה

ניתן לראות בתמונה בסעיף זה שהזיהות השולח והמקבל היא בדיקת הפוכה באיפי ובכחותה המאך, ובנוסף ניתן לראות בצד שמאל הח' שמחבר בין הודעה של התגובה להודעה המקורית שהלכה לשרת. התגובה מסומנת בכתרום בתמונה הראשונה

\*enp0s3

**dns**

No.	Time	Source	Destination	Protocol	Length	Info
36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.6779943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAM...

Frame 40: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0

Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5)

Internet Protocol Version 4, Src: 132.70.9.100, Dst: 10.0.2.15

User Datagram Protocol, Src Port: 53, Dst Port: 45651

Domain Name System (response)

```
0000  08 00 27 8b 4b c5 52 54 00 12 35 02 08 00 45 00  .'.K-RT ..5..E.
0010  00 6f be 96 00 00 40 11 22 2f 84 46 09 64 0a 00  .o...@. /-F-d..
0020  02 0f 00 35 b2 53 00 5b b6 41 70 cc 81 80 00 01  ..5 S [ Ap ...
0030  00 02 00 00 00 04 6f 63 73 70 08 64 69 67 69  .....o csp-digi
0040  63 65 72 74 03 63 6f 6d 00 00 01 00 01 c0 0c 00 cert.com .....
```

Ethernet (eth), 14 bytes

Packets: 14271 · Displayed: 838 (5.9%) · Dropped: 0 (0.0%) · Profile: Default

\*enp0s3

**dns**

No. Time Source Destination Protocol Length Info

36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.679943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAM...

Frame 40: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0

Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5)

Internet Protocol Version 4, Src: 132.70.9.100, Dst: 10.0.2.15

User Datagram Protocol, Src Port: 53, Dst Port: 45651

Domain Name System (response)

0020	02 0f 00 35 b2 53 00 5b b6 41 70 cc 81 80 00 01	...5-S-[ Ap...
0030	00 02 00 00 00 00 04 6f 63 73 70 08 64 69 67 69	....o csp-digi
0040	63 65 72 74 03 63 6f 6d 00 00 01 00 01 c0 0c 00	cert.com .....
0050	05 00 01 00 01 3d 09 00 14 03 63 73 39 03 77 61	....=... cs9-wa
0060	63 06 70 68 69 63 64 6e 03 6e 65 74 00 c0 2f 00	c-phicdn .net.../.

User Datagram Protocol (udp), 8 bytes

Packets: 14271 - Displayed: 838 (5.9%) - Dropped: 0 (0.0%) - Profile: Default

\*enp0s3

**dns**

No. Time Source Destination Protocol Length Info

36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.679943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAM...

Frame 40: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0

Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5)

Internet Protocol Version 4, Src: 132.70.9.100, Dst: 10.0.2.15

User Datagram Protocol, Src Port: 53, Dst Port: 45651

Domain Name System (response)

0000	08 00 27 8b 4b c5 52 54 00 12 35 02 08 00 45 00	...K RT . 5 . E.
0010	00 6f be 96 00 00 40 11 22 2f 84 46 09 64 0a 00	..o...@ "/.F.d..
0020	02 0f 00 35 b2 53 00 5b b6 41 70 cc 81 80 00 01	...5-S-[ Ap...
0030	00 02 00 00 00 04 6f 63 73 70 08 64 69 67 69	....o csp-digi
0040	63 65 72 74 03 63 6f 6d 00 00 01 00 01 c0 0c 00	cert.com .....

Internet Protocol Version 4 (ip), 20 bytes

Packets: 14271 - Displayed: 838 (5.9%) - Dropped: 0 (0.0%) - Profile: Default

\*enp0s3

**dns**

No.	Time	Source	Destination	Protocol	Length	Info
36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.679943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNM...

▶ Frame 40: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0

▶ Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5)

▶ Internet Protocol Version 4, Src: 132.70.9.100, Dst: 10.0.2.15

▶ User Datagram Protocol, Src Port: 53, Dst Port: 45651

▶ Domain Name System (response)

```

0000  08 00 27 8b 4b c5 52 54  00 12 35 02 08 00 45 00  .'.K.RT ..5..E.
0010  00 6f be 96 00 00 40 11  22 2f 84 46 09 64 0a 00  .o..@. "/-F-d-
0020  02 0f 00 35 b2 53 00 5b  b6 41 70 cc 81 80 00 01  ..5.S [ Ap....
0030  00 02 00 00 00 00 04 6f  63 73 70 08 64 69 67 69  ....o csp-digi
0040  63 65 72 74 03 63 6f 6d  00 00 01 00 01 c0 0c 00  cert.com .....

```

Ethernet (eth), 14 bytes

Packets: 14271 · Displayed: 838 (5.9%) · Dropped: 0 (0.0%) · Profile: Default

שעיף 1

\*enp0s3

**dns and ip.src==10.0.2.15**

No.	Time	Source	Destination	Protocol	Length	Info
36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
75	11.679943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
213	13.732058699	10.0.2.15	132.70.60.124	DNS	87	Standard query 0xb414 A safebrowsing.googleapis.com
240	13.800047111	10.0.2.15	132.70.60.124	DNS	85	Standard query 0xc40f A zdwidget3-bs.sphereup.com
241	13.800819954	10.0.2.15	132.70.60.124	DNS	85	Standard query 0x521d AAAA zdwidget3-bs.sphereup.com
256	13.829281255	10.0.2.15	132.70.60.124	DNS	82	Standard query 0xb43b A apv-launcher.minute.ly
257	13.829461474	10.0.2.15	132.70.60.124	DNS	82	Standard query 0x20c9 AAAA apv-launcher.minute.ly
261	13.840133422	10.0.2.15	132.70.60.124	DNS	82	Standard query 0x5301 A n3g6e9r8.ssl.hwcdn.net
262	13.840362749	10.0.2.15	132.70.60.124	DNS	82	Standard query 0x5426 AAAA n3g6e9r8.ssl.hwcdn.net
264	13.852098699	10.0.2.15	132.70.60.124	DNS	76	Standard query 0x975e A sf.exposebox.com
265	13.852326127	10.0.2.15	132.70.60.124	DNS	76	Standard query 0x8845 AAAA sf.exposebox.com

▶ Frame 37: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

▶ Ethernet II, Src: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 132.70.9.100

▶ User Datagram Protocol, Src Port: 45651, Dst Port: 53

Source Port: 45651

```

0000  52 54 00 12 35 02 08 00  27 8b 4b c5 08 00 45 00  RT..5... 'K..E.
0010  00 3f 8f 26 40 00 40 11  11 cf 0a 00 02 0f 84 46  .?&@.0. ....F
0020  09 64 b2 53 00 35 00 2b  99 f5 70 cc 01 00 00 01  .d.S.5.+ .p....
0030  00 00 00 00 00 00 04 6f  63 73 70 08 64 69 67 69  ....o csp-digi
0040  63 65 72 74 03 63 6f 6d  00 00 01 00 01 c0 0c 00  cert.com .....

```

User Datagram Protocol (udp), 8 bytes

Packets: 14271 · Displayed: 419 (2.9%) · Dropped: 0 (0.0%) · Profile: Default

עשינו סינון שהאינטרנט של המקרו יהיה האייפי של המחשב שלנו, ושהפרוטוקול יהיה dns

\*enp0s3

**DNS and TCP.pcap** 10.0.2.15 Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAM...
215	13.735701930	132.70.60.124	10.0.2.15	DNS	103	Standard query response 0xb414 A safebrowsing.googleapis...
258	13.831060683	132.70.60.124	10.0.2.15	DNS	150	Standard query response 0xb43b A apv-launcher.minute.ly C...
259	13.831621875	132.70.60.124	10.0.2.15	DNS	175	Standard query response 0x20c9 AAAA apv-launcher.minute.l...
263	13.843974596	132.70.60.124	10.0.2.15	DNS	98	Standard query response 0x5301 A n3g6e9r8.ssl.hwcdn.net A...
266	13.853966292	132.70.60.124	10.0.2.15	DNS	92	Standard query response 0x975e A sf.exposebox.com A 35.18...
267	13.868389958	132.70.60.124	10.0.2.15	DNS	144	Standard query response 0x8845 AAAA sf.exposebox.com SOA ...
268	13.869492989	132.70.60.124	10.0.2.15	DNS	290	Standard query response 0xc40f A zdwidget3-bs.sphereup.co...
291	13.914203217	132.70.60.124	10.0.2.15	DNS	139	Standard query response 0x5426 AAAA n3g6e9r8.ssl.hwcdn.ne...
326	14.024756182	132.70.60.124	10.0.2.15	DNS	347	Standard query response 0x521d AAAA zdwidget3-bs.sphereup...

► Frame 38: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0

► Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5)

► Internet Protocol Version 4, Src: 132.70.60.124, Dst: 10.0.2.15

▼ User Datagram Protocol, Src Port: 53, Dst Port: 45651

Source Port: 53

```
0020 02 0f 00 35 b2 53 00 5b 5f 29 70 cc 81 80 00 01  .+5.S.[ ]p.....
0030 00 02 00 00 00 00 04 6f 63 73 70 08 64 69 67 69  .....o csp.digi
0040 63 65 72 74 03 63 6f 6d 00 00 01 00 01 c0 0c 00 cert.com .....
0050 05 00 01 00 01 3d 28 00 14 03 63 73 39 03 77 61  ....=(. .cs9-wa
0060 63 06 70 68 69 63 64 6e 03 6e 65 74 00 c0 2f 00 c-phicdn .net..../
```

\_packets: 14271 · \_displayed: 419 (2.9%) · \_dropped: 0 (0.0%) · \_profile: Default

ישנו סינון שהאיפי של היעד היה האיפי של המחשב שלנו, וההפרוטוקול היה dns  
ניתן ללמוד מסעיף זה שהפורט של שרת dns הוא פорт 53

**סעיף נ**

\*enp0s3

**udp.srcport==53 or udp.dstport==53** Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
36	9.372339156	10.0.2.15	132.70.60.124	DNS	77	Standard query 0x70cc A ocsp.digicert.com
37	9.372477050	10.0.2.15	132.70.9.100	DNS	77	Standard query 0x70cc A ocsp.digicert.com
38	9.375204577	132.70.60.124	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
40	9.377300978	132.70.9.100	10.0.2.15	DNS	125	Standard query response 0x70cc A ocsp.digicert.com CNAME ...
47	9.552134017	10.0.2.15	132.70.60.124	DNS	72	Standard query 0xdcd9 A sport5.co.il
48	9.552310363	10.0.2.15	132.70.60.124	DNS	72	Standard query 0x46f3 AAAA sport5.co.il
49	9.554091123	132.70.60.124	10.0.2.15	DNS	88	Standard query response 0xdcd9 A sport5.co.il A 82.166.10...
50	9.559534122	132.70.60.124	10.0.2.15	DNS	137	Standard query response 0x46f3 AAAA sport5.co.il SOA dns...
75	11.679943705	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xbb5e A tiles.services.mozilla.com
76	11.680115860	10.0.2.15	132.70.60.124	DNS	86	Standard query 0xc983 AAAA tiles.services.mozilla.com
77	11.680583458	10.0.2.15	132.70.60.124	DNS	86	Standard query 0x4213 A tiles.services.mozilla.com
78	11.683923693	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0xbb5e A tiles.services.mozilla.c...
79	11.686293558	132.70.60.124	10.0.2.15	DNS	194	Standard query response 0xc983 AAAA tiles.services.mozilla...
80	11.688270719	132.70.60.124	10.0.2.15	DNS	240	Standard query response 0x4213 A tiles.services.mozilla.c...
94	12.113563729	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xeb96 A www.sport5.co.il
95	12.113876437	10.0.2.15	132.70.60.124	DNS	76	Standard query 0xe36b AAAA www.sport5.co.il
96	12.115915388	132.70.60.124	10.0.2.15	DNS	106	Standard query response 0xeb96 A www.sport5.co.il CNAME s...
97	12.116476555	132.70.60.124	10.0.2.15	DNS	155	Standard query response 0xe36b AAAA www.sport5.co.il CNAM...

► Frame 38: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0

► Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_8b:4b:c5 (08:00:27:8b:4b:c5)

► Internet Protocol Version 4, Src: 132.70.60.124, Dst: 10.0.2.15

▼ User Datagram Protocol, Src Port: 53, Dst Port: 45651

Source Port: 53

```
0020 02 0f 00 35 b2 53 00 5b 5f 29 70 cc 81 80 00 01  .+5.S.[ ]p.....
0030 00 02 00 00 00 00 04 6f 63 73 70 08 64 69 67 69  .....o csp.digi
0040 63 65 72 74 03 63 6f 6d 00 00 01 00 01 c0 0c 00 cert.com .....
0050 05 00 01 00 01 3d 28 00 14 03 63 73 39 03 77 61  ....=(. .cs9-wa
0060 63 06 70 68 69 63 64 6e 03 6e 65 74 00 c0 2f 00 c-phicdn .net..../
```

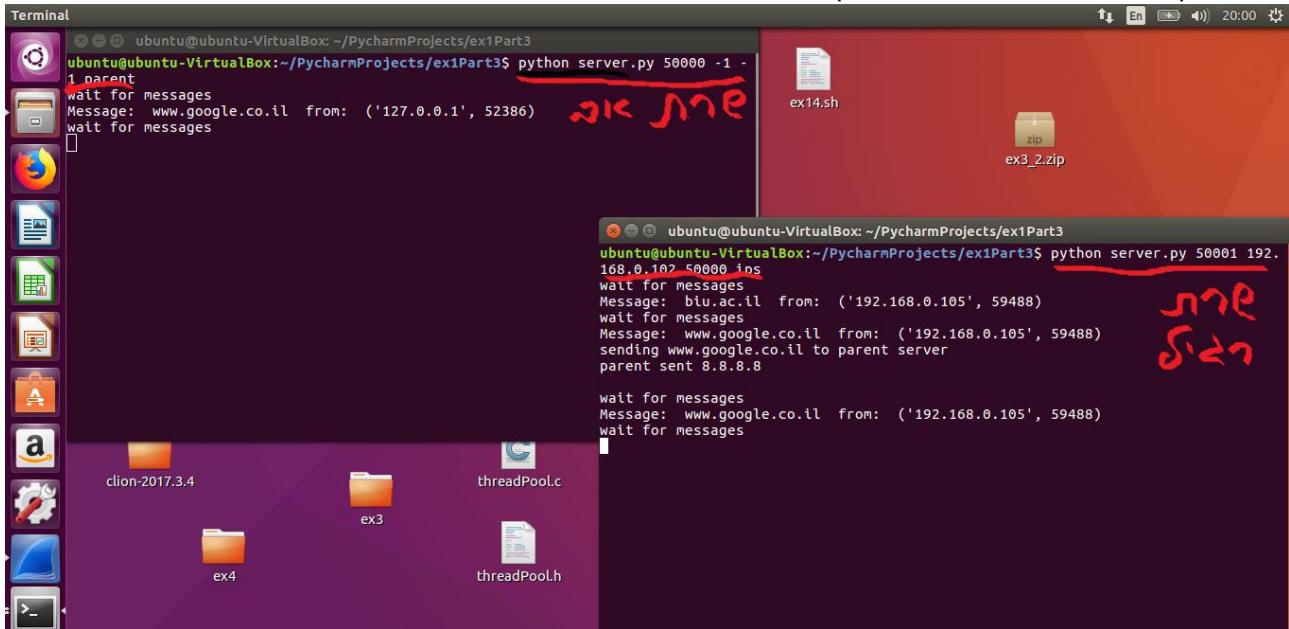
\_packets: 14271 · \_displayed: 838 (5.9%) · \_dropped: 0 (0.0%) · \_profile: Default

ובצע סינון לפי פорт 53 כפורת של המקור או של היעד

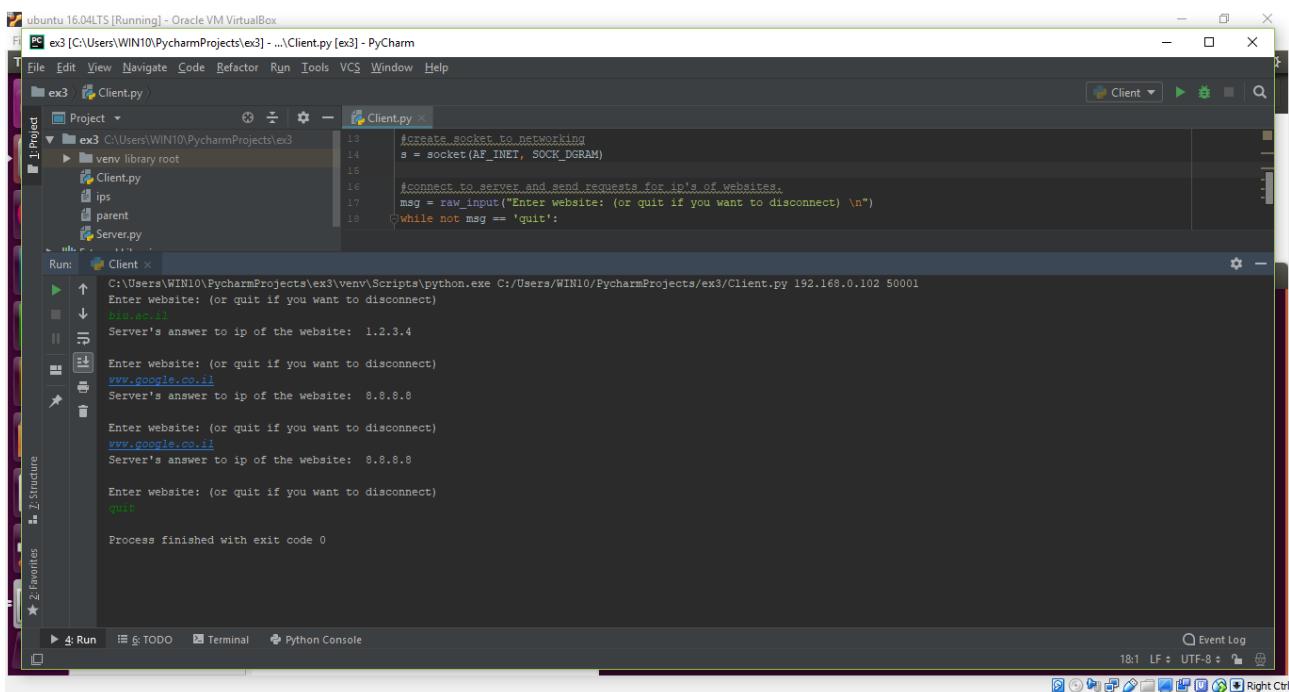
### 3: שאלה

דוגמת הריצה ב 2 מכונות שונות:

צד שרת: (2) הסרברים – מכונה וירטואלית



צד לקוח: (וינדוס)



### תיאור דוגמת הרצאה:

ניתן לראות בשתי התמונות, שהרצינו ב 2 מכונות שונות, שבתחלת הלקוח מבקש את האתר\* [www.biu.ac.il](http://www.biu.ac.il)

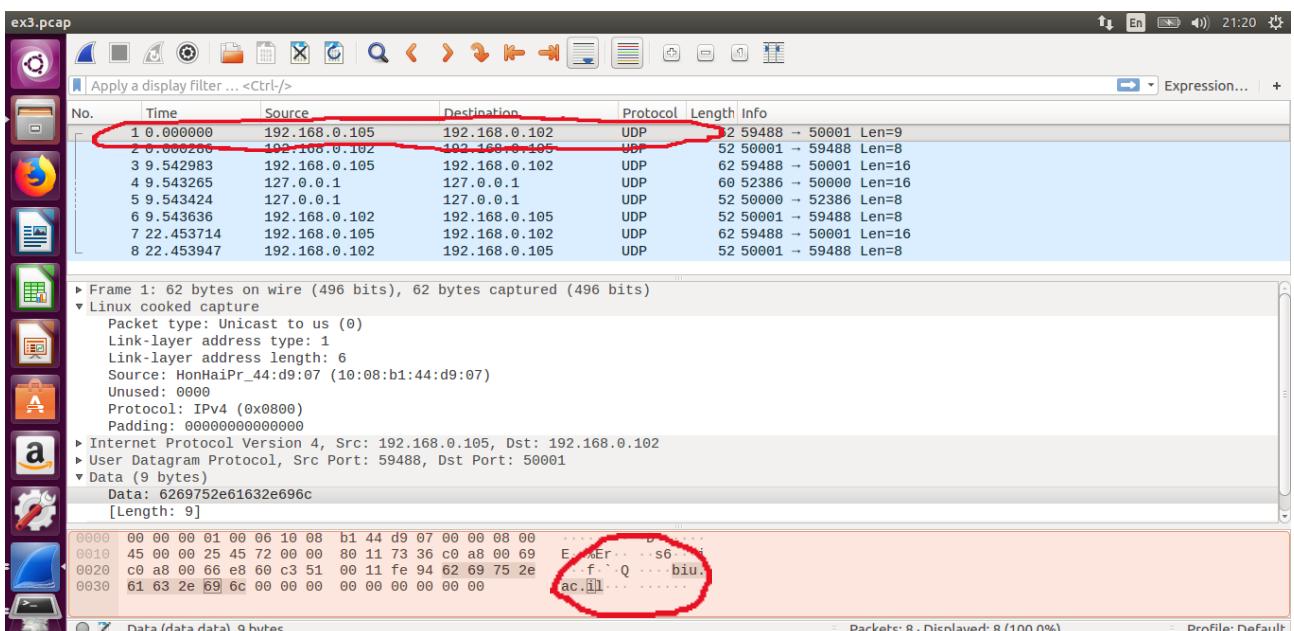
שרת הבן מחזיר לו את התשובה.

לאחר מכן, הלקוח מבקש את\* [www.google.co.il](http://www.google.co.il) לשרת הבן אין את הכתובת בקובץ שלו ולכון הוא מבקש משרת האב את המידע שמחזיר לו את המידע, ושרת הבן שולח את המידע ללקוח.

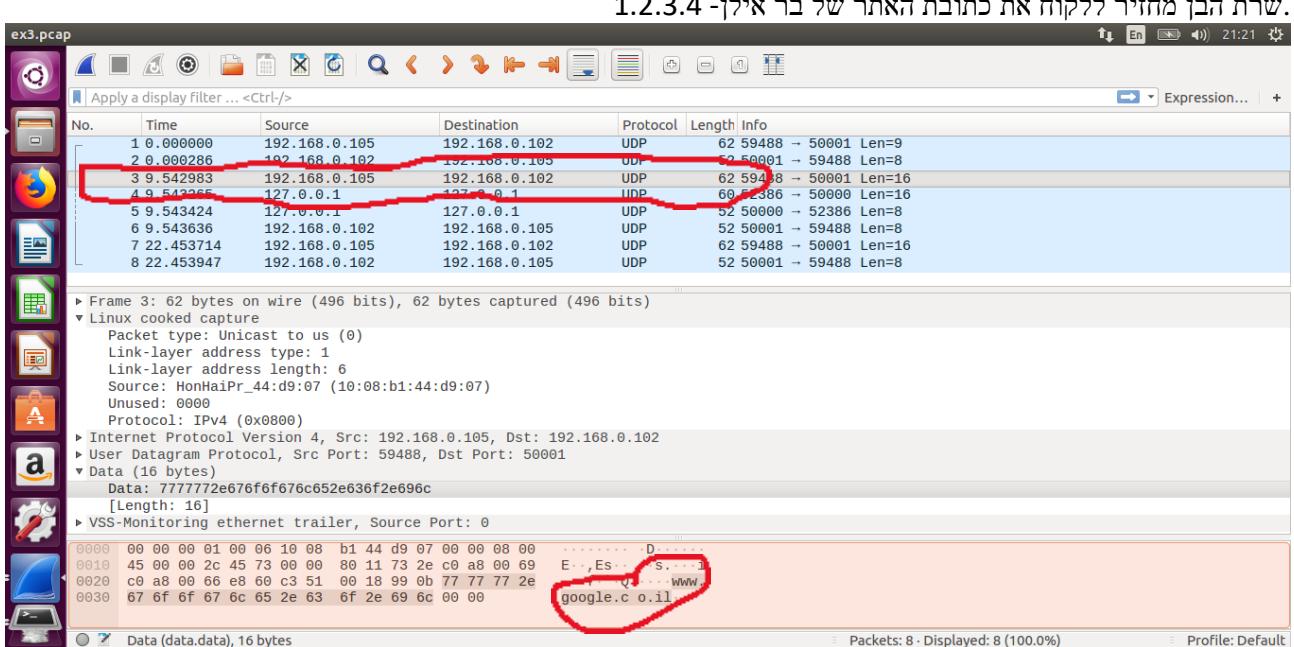
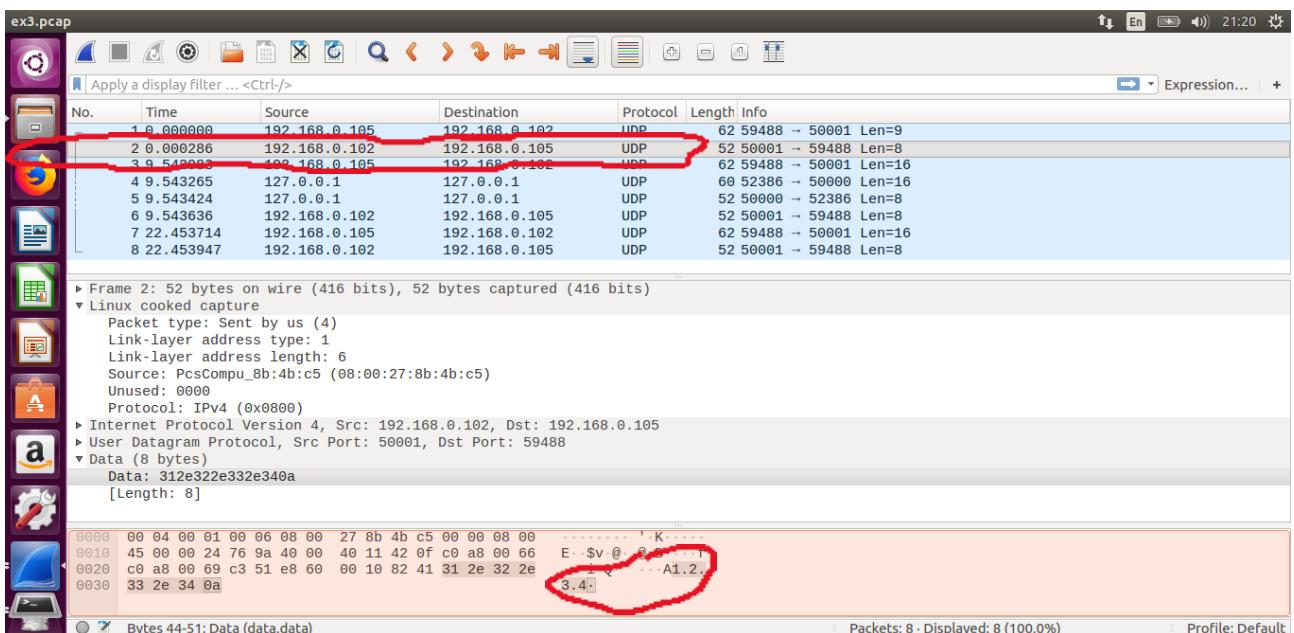
בפעם השלישייה הלקוח מבקש שוב את\* [www.google.co.il](http://www.google.co.il) לשרת הבן כבר יש את הכתובת במאגר מהבקשת הקודמת ולכון הוא שולח ישר את התשובה ללקוח(לא התערבות של שרת האב).

כתובת הלקוח – 10.0.2.15  
כתובת השרת – 172.19.3.206

### WIRESHARK:



בחבילת הראשונה- הלקוח שולח בקשה לשרת לקבל את האתר של בר אילן.



הלקוח מבקשת את גוגל (תזכורת : השרת הרגיל שלנו לא מכיר את האתר של גוגל).

Screenshot of Wireshark showing network traffic. A red box highlights the fourth packet (Frame 4) which is a UDP request from 127.0.0.1 to 127.0.0.102. Another red box highlights the data bytes 0030 through 0033, which show the domain name "google.co.il".

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.105	192.168.0.102	UDP	62	59488 → 50001 Len=9
2	0.000286	192.168.0.102	192.168.0.105	UDP	52	50001 → 59488 Len=8
3	0.542522	192.168.0.105	192.168.0.102	UDP	62	59488 → 50001 Len=16
4	9.543265	127.0.0.1	127.0.0.1	UDP	60	52386 → 50000 Len=16
5	9.543424	127.0.0.1	127.0.0.1	UDP	52	50000 → 52386 Len=8
6	9.543636	192.168.0.102	192.168.0.105	UDP	52	50001 → 59488 Len=8
7	22.453714	192.168.0.105	192.168.0.102	UDP	62	59488 → 50001 Len=16
8	22.453947	192.168.0.102	192.168.0.105	UDP	52	50001 → 59488 Len=8

Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
 ▾ Linux cooked capture  
 ▸ Packet type: Unicast to us (0)  
 Link-layer address type: 772  
 Link-layer address length: 6  
 Source: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
 Unused: 0000  
 Protocol: IPv4 (0x0800)  
 ▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
 ▸ User Datagram Protocol, Src Port: 52386, Dst Port: 50000  
 ▾ Data (16 bytes)  
 Data: 777772e676f6f676c652e636f2e696c [Length: 16]

0000 00 00 03 04 00 06 00 00 00 00 00 00 00 00 08 00 . . . . . . . .  
 0010 45 00 00 2c bd bb 40 00 40 11 7f 03 7f 00 00 01 E - , . @ . . . . . . .  
 0020 7f 00 00 01 cc a2 c3 50 00 18 fe 2b 77 77 77 2e . . . . . . . . . . . . .  
 0030 67 6f 6f 67 6c 65 2e 63 6f 2e 69 6c google.co.il [Length: 16]

Bytes 44-59: Data (data.data)

כאן ניתן לראות שכיוון שהשרת הרגיל אינו מכיר את האתר גוגל, הוא פונה לשרת האב על מנת שהוא ייתן לו את הכתובת של האתר גוגל.

Screenshot of Wireshark showing network traffic. A red box highlights the fourth packet (Frame 5) which is a UDP response from 127.0.0.1 to 127.0.0.102. Another red box highlights the data bytes 0030 through 0033, which show the IP address "8.8.8.8".

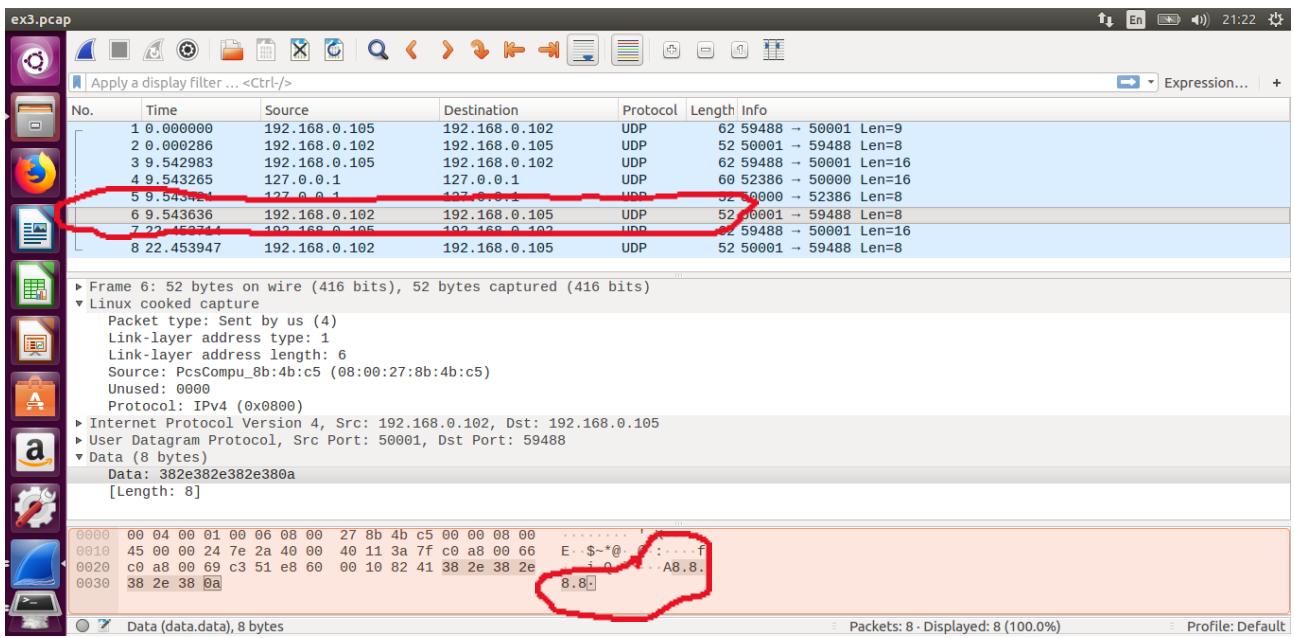
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.105	192.168.0.102	UDP	62	59488 → 50001 Len=9
2	0.000286	192.168.0.102	192.168.0.105	UDP	52	50001 → 59488 Len=8
3	0.542522	192.168.0.105	192.168.0.102	UDP	62	59488 → 50001 Len=16
4	9.543265	127.0.0.1	127.0.0.1	UDP	60	52386 → 50000 Len=16
5	9.543424	127.0.0.1	127.0.0.1	UDP	52	50000 → 52386 Len=8
6	9.543636	192.168.0.102	192.168.0.105	UDP	52	50001 → 59488 Len=8
7	22.453714	192.168.0.105	192.168.0.102	UDP	62	59488 → 50001 Len=16
8	22.453947	192.168.0.102	192.168.0.105	UDP	52	50001 → 59488 Len=8

Frame 5: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)  
 ▾ Linux cooked capture  
 ▸ Packet type: Unicast to us (0)  
 Link-layer address type: 772  
 Link-layer address length: 6  
 Source: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
 Unused: 0000  
 Protocol: IPv4 (0x0800)  
 ▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
 ▸ User Datagram Protocol, Src Port: 50000, Dst Port: 52386  
 ▾ Data (8 bytes)  
 Data: 382e382e382e380a [Length: 8]

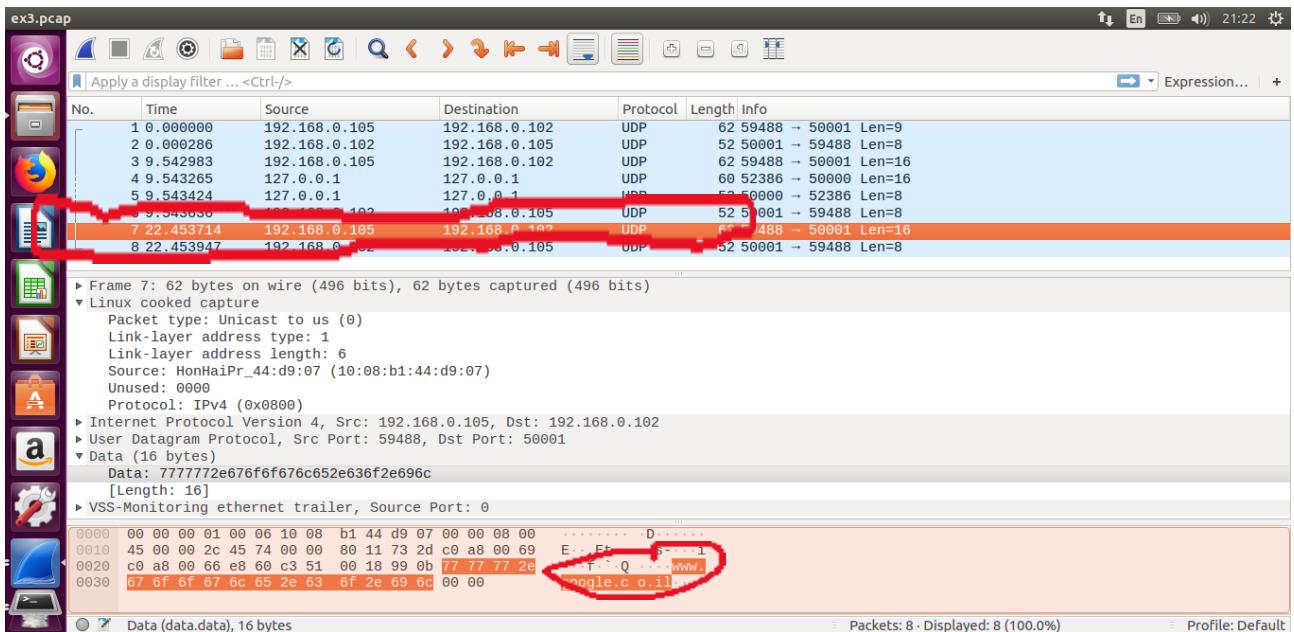
0000 00 00 03 04 00 06 00 00 00 00 00 00 00 00 08 00 . . . . . . . .  
 0010 45 00 00 24 bd bc 40 00 40 11 7f 0a 7f 00 00 01 E - \$ - @ . . . . . . .  
 0020 7f 00 00 01 c3 50 cc a2 00 10 fe 23 38 2e 38 2e . . . . . . . . . . .  
 0030 38 2e 38 0a 8.8.8.8

Data (data.data), 8 bytes

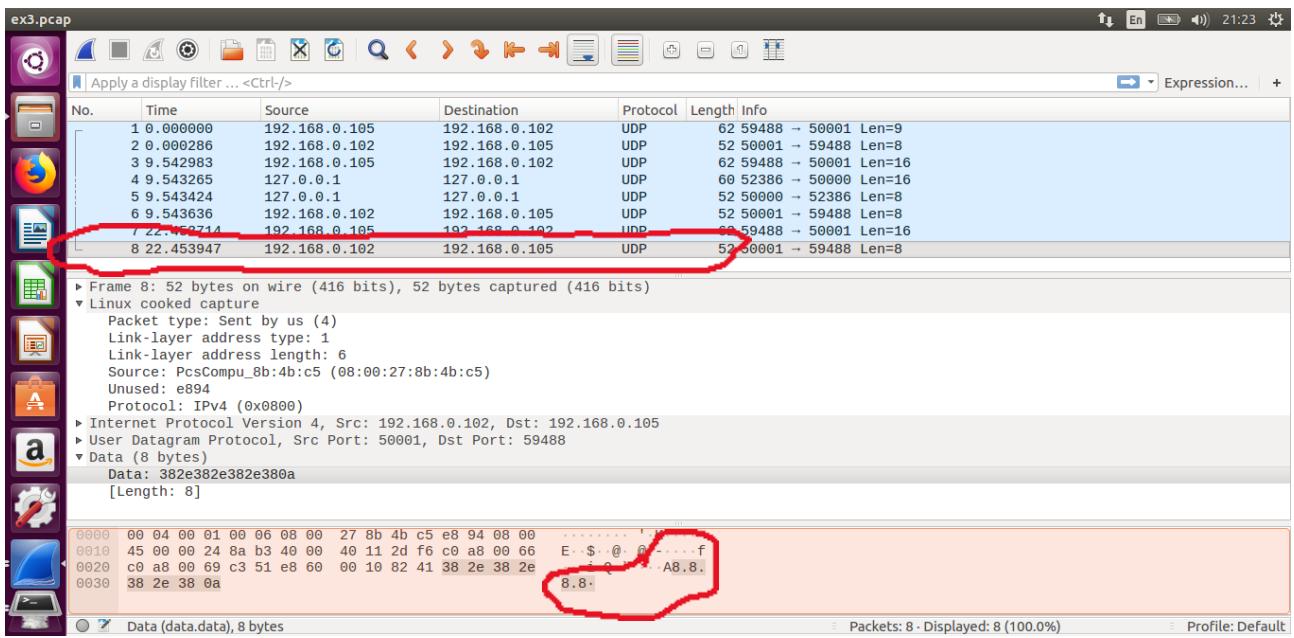
כאן שרת האב מקבל את הבקשה מהשרת הרגיל, והוא מכיר את האתר גוגל והוא שולח לשרת הרגיל את הכתובת של גוגל.



שרת הבן שולח חוזה ללקוח את הכתובת של גוגל **שיהי 8.8.8.8** לאחר שקיבל אותה משרת האב.



כעת הלוקה מבקששוב מהשרת את אתר גוגל



..וכעת השרת כבר מכיר את כתובתה של אתר גוגל ולכן ישר שולח ללקוחה

#### דגשין:

ניתן לראות כי כל פאקטה כוללת רק כתובת מק אחת שהיא כתובת המקור בכל פאקטה יש פירוט של שכבה הילינק(השכבה ה2) , השכבה ה3 שומרה את כתובת איפי מקור ויעד , והשכבה ה4 שומרה את הפורט מקור ויעד.